



Copia de seguridad y restauración de Elasticsearch



m:
<https://pandorafms.com/manual/!current/>
Permanent link:
https://pandorafms.com/manual/!current/es/documentation/pandorafms/technical_annexes/16_elastic_search_backup
2024/06/10 14:36



Copia de seguridad y restauración de Elasticsearch

La migración de datos de un servidor Elasticsearch mediante *snapshots* se realiza con relativa rapidez. En primer lugar, se realiza una copia de seguridad de los datos del servidor y después se guarda en un repositorio para posterior restauración del mismo.

Crear copia de Seguridad

La máquina donde se realizará el *backup* se denomina “máquina origen” y la máquina donde se realizará la restauración se denomina “máquina destino”.

- En la máquina origen

Modifique el fichero de configuración `elasticsearch.yml`:

```
vi /etc/elasticsearch/elasticsearch.yml
```

Añada la siguiente línea:

```
path.repo: /usr/local/var/backups/
```

Cree el directorio añadido anteriormente al fichero de configuración:

```
mkdir -p /usr/local/var/backups/
```

Otorgue permisos de lectura y escritura al directorio y usuario:

```
chmod 700 /usr/local/var/backups  
chown elasticsearch:elasticsearch /usr/local/var/backups
```

Reinicie servicio:

```
/etc/init.d/elasticsearch restart
```

Cree *backup*:

```
curl -XPUT http://localhost:9200/_snapshot/my_backup -d '{"type": "fs",  
"settings": {"compress": "true", "location": "/usr/local/var/backups/"}}'
```

Comprima *backup*:

```
cd /usr/local/var/  
tar -zcvf elastic_backup.tar.gz backups/
```

Desde la máquina destino copie el *backup* comprimido de la máquina origen.

```
scp -P 41122 root@<dir_ip_origin>:/root/elastic_backup.tar.gz /home/user/backup
```

- Para utilizar el comando `scp` se debe tener instalado un servidor SSH en la máquina origen y al menos un cliente SSH en la máquina destino.
- Es importante que la versión de Elasticsearch en la máquina destino sea compatible con la exportación de datos; es decir, en este caso la máquina origen debe tener la misma versión o superior. Si no es así, primero debe actualizar Elasticsearch en la máquina destino.

Restaurar copia de Seguridad

- En la máquina destino.

Modificar el fichero de configuración `elasticsearch.yml` de la misma manera hecha al crear el *backup* en la máquina origen:

```
vi /etc/elasticsearch/elasticsearch.yml
```

Añadir la siguiente línea:

```
path.repo: /usr/local/var/backups/
```

Crear el directorio añadido anteriormente al fichero de configuración:

```
mkdir -p /usr/local/var/backups/
```

Otorgar permisos de lectura y escritura al directorio:

```
chmod 700 /usr/local/var/backups  
chown elasticsearch:elasticsearch /usr/local/var/backups
```

Reiniciar el servicio:

```
/etc/init.d/elasticsearch restart
```

Descomprimir el *backup* importado de la máquina origen:

```
tar -xzvf /home/user/backup/elastic_backup.tar.gz -C /usr/local/var/backups
```

Crear los repositorios donde se localizan las *snapshots*:

```
curl -X PUT "localhost:9200/_snapshot/my_backup" -H 'Content-Type: application/json' -d '{
  "type": "fs",
  "settings": {
    "location": "/usr/local/var/backups"
  }
}'
```

Cerrar los índices:

```
curl -XPOST http://localhost:9200/<nombreIndice>-*/_close
```

El asterisco muestra todos los índices que empiecen por ese nombre.

Importar el *backup*: Primero copiar el *backup* al repositorio:

```
cp <name_snapshot.dat> my_backup_location/
```

Renombrar el fichero sin mayúsculas:

```
mv my_backup_location/<name_snapshot.dat> my_backup_location/snap1
```

Finalmente se importa:

```
curl -X POST
"localhost:9200/_snapshot/my_backup/snap1/_restore?wait_for_completion=true"
```

Para terminar, reabrir los índices:

```
curl -XPOST http://localhost:9200/<nombreIndice>-*/_open
```

[Volver al Índice de Documentación Pandora FMS](#)